

Vice Society spreads its own ransomware

By Intrinsec

Published: 2023-02-14 · Archived: 2026-04-06 01:17:05 UTC



[CERT Intrinsec Incidents Report 2025](#)

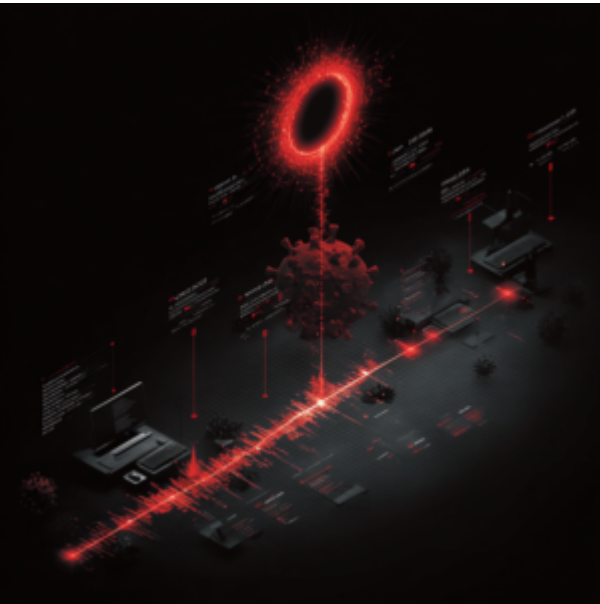
février 24, 2026 Aucun commentaire

CERT Intrinsec is a French Incident Response team providing incident response and crisis management services to organizations across multiple sectors. Certified PRIS (Prestataire de Réponse aux Incidents de Sécurité) by ANSSI since 2022, the team has been operating since 2013 and has handled hundreds of engagements, gaining firsthand insight into the evolution of threat actor tradecraft.

In 2025, CERT Intrinsec was engaged in approximately sixty significant incidents involving ransomware operators, Initial Access Brokers (IABs), insider threats, and suspected state-sponsored actors conducting intelligence operations. These incidents spanned a wide range of environments, from legacy on-premise infrastructure to cloud-native Microsoft 365 tenants.

This report synthesizes our observations from these engagements with a focus on actionable findings. Rather than presenting descriptive statistics alone, we examine intrusion mechanisms, attacker dwell time, targeted assets, and defensive gaps — with the explicit goal of informing detection strategies and hardening priorities for security practitioners.

[Lire](#)





[CERT Intrinsec Incidents Report 2025](#)

février 24, 2026 Aucun commentaire

CERT Intrinsec is a French Incident Response team providing incident response and crisis management services to organizations across multiple sectors. Certified PRIS (Prestataire de Réponse aux Incidents de Sécurité) by ANSSI since 2022, the team has been operating since 2013 and has handled hundreds of engagements, gaining firsthand insight into the evolution of threat actor tradecraft.

In 2025, CERT Intrinsec was engaged in approximately sixty significant incidents involving ransomware operators, Initial Access Brokers (IABs), insider threats, and suspected state-sponsored actors conducting intelligence operations. These incidents spanned a wide range of environments, from legacy on-premise infrastructure to cloud-native Microsoft 365 tenants.

This report synthesizes our observations from these engagements with a focus on actionable findings. Rather than presenting descriptive statistics alone, we examine intrusion mechanisms, attacker dwell time, targeted assets, and defensive gaps — with the explicit goal of informing detection strategies and hardening priorities for security practitioners.

[Lire](#)





Source: <https://www.intrinsec.com/vice-society-spreads-its-own-ransomware/>